

1    CLAIMS

2    What is claimed is:

3        1.     A method comprising:  
4        determining if a smartcard is operatively available, said smartcard having  
5        smartcard memory;  
6        identifying at least one root certificate stored in said smartcard memory;  
7        and  
8        reading said at least one root certificate from said smartcard memory.

9  
10       2.     The method as recited in Claim 1, further comprising:  
11       storing said at least one root certificate in a device operatively coupled to  
12       said smartcard.

13  
14       3.     The method as recited in Claim 2, wherein said device includes a  
15       computing device having computer memory, and wherein storing said at least one  
16       root certificate in said device operatively coupled to said smartcard further  
17       includes:

18       adding said at least one root certificate to a certificate store maintained in  
19       said computer memory.

20  
21       4.     The method as recited in Claim 1, wherein identifying said at least  
22       one root certificate stored in said smartcard memory further includes  
23       authenticating information associated with said smartcard prior to identifying said  
24       at least one root certificate.

25

1           5.     The method as recited in Claim 2, further comprising:  
2           determining when said smartcard is no longer operatively available; and  
3           no longer storing said root certificate in said device when said smartcard is  
4           no longer operatively available.

5  
6           6. The method as recited in Claim 2, further comprising:  
7           determining when an account associated with said smartcard is not active;  
8           and  
9           no longer storing said root certificate in said device when said account is  
10          not active.

11  
12          7.     The method as recited in Claim 6, wherein said account is associated  
13          with a user and determining when said account is not active includes determining  
14          is said user is currently logged on.

15  
16          8.     The method as recited in Claim 5, wherein no longer storing said  
17          root certificate in said device when said smartcard is no longer operatively  
18          available includes:

19                removing said stored root certificate from a certificate store maintained in  
20                computer memory of said device.

21  
22          9.     A computer readable medium having computer-implementable  
23          instructions for causing one or more processing units to perform acts comprising:

24                determining if a smartcard, having smartcard memory with at least one root  
25                certificate stored therein, is operatively available; and

1 reading said at least one root certificate from said smartcard memory.  
2

3 10. The computer readable medium as recited in Claim 9, having further  
4 computer-implementable instructions for causing one or more processing units to  
5 perform acts comprising:

6 storing said at least one root certificate in a device operatively coupled to  
7 said smartcard.  
8

9 11. The computer readable medium as recited in Claim 10, having  
10 further computer-implementable instructions for causing one or more processing  
11 units to perform acts comprising:

12 adding said read root certificate to a certificate store maintained in  
13 computer memory of said device.  
14

15 12. The computer readable medium as recited in Claim 9, having further  
16 computer-implementable instructions for causing one or more processing units to  
17 perform acts comprising:

18 authenticating information associated with said smartcard prior to reading  
19 said at least one root certificate.  
20

21 13. The computer readable medium as recited in Claim 10, further  
22 comprising:

23 determining when said smartcard is no longer operatively available; and  
24 no longer storing said root certificate in said device when said smartcard is  
25 no longer operatively available.

1  
2 14. The computer readable medium as recited Claim 10, further  
3 comprising:

4 determining when an account associated with said smartcard is not active;  
5 and

6 no longer storing said root certificate in said device when said account is  
7 not active.  
8

9 15. The method as recited in Claim 14, wherein said account is  
10 associated with a user and determining when said account is not active includes  
11 determining is said user is currently logged on.  
12

13 16. The computer readable medium as recited in Claim 13, wherein no  
14 longer storing said root certificate in said device when said smartcard is no longer  
15 operatively available includes:

16 removing said stored root certificate from a certificate store maintained in  
17 computer memory of said device.  
18

19 17. A system comprising:

20 a computing device having computer memory;

21 a smartcard interface device operatively coupled to said computing device  
22 and configurable to operatively interface to a smartcard, having smartcard memory  
23 with at least one root certificate stored therein; and

24 wherein said computing device includes logic configured to identify when  
25 said smartcard is operatively available via said smartcard interface device, identify

1 said root certificate in said smartcard memory, and cause said smartcard interface  
2 device to read said identified root certificate from said smartcard memory and  
3 provide said root certificate to said logic.

4  
5 18. The system as recited in Claim 17, wherein said logic is further  
6 configured to store said root certificate in a certificate store maintained in said  
7 computer memory.

8  
9 19. The system as recited in Claim 17, wherein said logic is further  
10 configured to authenticate information associated with said smartcard prior to  
11 causing said smartcard interface device to read said root certificate.

12  
13 20. The computer readable medium as recited in Claim 18, wherein said  
14 logic is further configured to determine when said smartcard is no longer  
15 operatively available, and remove said root certificate in said certificate store  
16 when said smartcard is no longer operatively available.

17  
18 21. A method comprising:  
19 determining if a smartcard is operatively available, said smartcard having  
20 smartcard memory; and  
21 storing at least one root certificate in said smartcard memory.

22  
23 22. The method as recited in Claim 21, further comprising:  
24 authenticating information associated with said smartcard prior to storing  
25 said at least one root certificate in said smartcard memory.

1  
2 23. A computer readable medium having computer-implementable  
3 instructions for causing one or more processing units to perform acts comprising:  
4 identifying when a smartcard is operatively available, said smartcard  
5 having smartcard memory; and  
6 storing at least one root certificate in said smartcard memory.  
7

8 24. The computer readable medium as recited in Claim 23, having  
9 further computer-implementable instructions for causing one or more processing  
10 units to perform acts comprising:  
11 authenticating information associated with said smartcard prior to storing  
12 said at least one root certificate in said smartcard memory.  
13

14 25. An apparatus comprising logic configured to identify when a  
15 smartcard is operatively available, said smartcard having smartcard memory, and  
16 store at least one root certificate in said smartcard memory.  
17

18 26. The apparatus as recited in Claim 25, wherein said logic is further  
19 configured to authenticate information associated with said smartcard prior to  
20 storing said at least one root certificate in said smartcard memory.  
21

22 27. A method comprising:  
23 determining if a smartcard is operatively available, said smartcard having  
24 smartcard memory with at least one root certificate stored therein; and  
25 removing said at least one root certificate from said smartcard memory.

1  
2        28.    The method as recited in Claim 27, further comprising:  
3        authenticating information associated with said smartcard prior to removing  
4        said at least one root certificate from said smartcard memory.

5  
6        29.    A computer readable medium having computer-implementable  
7        instructions for causing one or more processing units to perform acts comprising:  
8        identifying if a smartcard is operatively available, said smartcard having  
9        smartcard memory with at least one root certificate stored therein; and  
10       removing said at least one root certificate from said smartcard memory.

11  
12       30.    The computer readable medium as recited in Claim 29, having  
13       further computer-implementable instructions for causing one or more processing  
14       units to perform acts comprising:  
15       authenticating information associated with said smartcard prior to removing  
16       said at least one root certificate from said smartcard memory.

17  
18       31.    An apparatus comprising logic configured to identify when a  
19       smartcard is operatively available, said smartcard having smartcard memory with  
20       at least one root certificate stored therein, and remove said at least one root  
21       certificate from said smartcard memory.

22  
23       32.    The apparatus as recited in Claim 31, wherein said logic is further  
24       configured to authenticate information associated with said smartcard prior to  
25       removing said at least one root certificate from said smartcard memory.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

33. A smartcard having memory in which at least one root certificate is stored.